基于 GPRS 的远程监控系统的安全问题研究

Research on Security of Remote Power Supervisory System Based on GPRS

黄燕青 （厦门大学信息科学与技术学院自动化系，福建 厦门 361005）

摘 要

简单介绍基于 GPRS 和 Internet 的电力监控系统的设计结构，着重分析了影响 GPRS 系统安全的因素以及系统在运行中所面临的安全威胁，并在此基础上结合 GPRS 系统的特点，提出了保障系统通信正常及数据传输安全的技术策略。

关键词：GPRS，监控系统，系统安全

Abstract

This paper briefly introduces the design structure of electric power supervisory system based on GPRS and Internet technology.It focuses on analyzing the influencing factors of system security and security threat faced of the system in running.On this basis,combining character of GPRS system,this paper puts forward the technology strategies to guarantee the normal operation of system communication and the security of data transmission.

Keywords:GPRS,supervisory system,system security

基于 GPRS 网络数据传输的安全性问题一直困扰着运营商和电力用户，如何在保证 GPRS 网络快速、准确传输电力系统数据的同时确保传输数据与系统的安全性是一个急待解决的难题。

1 监控系统的组成

基于 GPRS 技术的远程监控系统由监控中心的主站端计算机，多台远程监控终端，中继站和 GPRS 网络构成。

监控中心实时接收每个箱式变电站的主动上发数据，并进行数据分析，将分析结果显示在监控界面上。同时将不同的数据分类保存到数据库中，以便监控人员随时查看。如有异常状况就启动报警，并在监控系统中保留报警记录。监控中心还可以观察每个箱式变电站的 DTU 和 RTU 工作情况。除了监测方面，监控中心还可以实时控制每个箱式变电站的路灯的开启和关闭。

中继站是为整个监控系统的通信提供中转功能，它需要接入到移动内网的固定 IP 地址。而主站和子站只需要与 DTU 连接，就可以与中继站通信。中继站采用 Visual C++的 Socket 编程。

监控终端（子站）负责监视每条电缆的运行情况和每个箱式变电站的门开启和闭合情况，并通过 DTU 周期性的将这些监控数据以及所有回路的电流、电压等信息主动上发至监控中心，当主站有报文下送时，监控终端分析这些命令，并执行相应动作。

主站与子站之间的数据通信规约采用 CDT（循环式远动）规约，该规约是我国电力部门进行电力调度和电力监控所使用的规约，用途十分广泛。CDT 规约的一帧报文一般分为三个部分：同步字、控制字、信息字。同步字：3 组 D7 09H。控制字：有六个字节分为控制字节，帧类别，信息字数 n，源站址，目地站址，校验码。其中控制字节定义和帧类别定义限于篇幅不进行详述；信息字数为包含信息字的个数；源站址即各个子站的 ID 号，用以区别各个子站；目的站址即主站的 ID 号；CRC 校验码采用 8 位 CRC 校验。

2 监控系统安全性分析

基于 GPRS 的远程监控方案由于其高效性和实用性，在越来越多的远程监控系统中被广泛采用。但是由于 GPRS 技术的特点，GPRS 网络自身也存在一些安全缺陷。电力监控系统直接控制道路、桥梁等相关的照明和景观亮化设施，能否正常稳定的运行关系重大，而系统主站和子站间的数据通信是整个系统运行的根本，因此系统数据传输的安全性是一个至关重要的问题。基于 GPRS 监控系统的安全性主要面临以下几方面的威胁：

2.1 GPRS 网络部分的因素

作为 GPRS 网的移动数据 IP 接入网承载在现有的 GSM 网上，网络本身存在一些列安全问题，如身份认证问题、信令及数据加密问题、SIM 卡问题和其他安全问题。基于 GSM 网络的 GPRS 网络继承了 GSM 网络的有效的安全机制，同时比 GSM 网络有所提高，表现在用户数据和信令的加密上，降低了明文传输的范围。但是 GPRS 网络毕竟是在 GSM 网络基础上通过增加特定的网络设备构建起来的，所以必然存在 GSM 网络在安全方面的一些缺陷，所以在利用 GPRS 进行安全通信时，不能只依靠 GPRS 系统本身的安全机制，还应在应用层上加强安全保护。

2.2 计算机系统部分的因素

整个系统的监控软件分别安装在上位工控机上和下位机子站中，中继系统也安装在中继计算机上，因此计算机系统稳定与否直接关系到整个监控系统的正常运行，如果计算机系统遭受网络攻击、断电或出现死机等状况，监控系统将失去作用，同时要保证系统数据库的安全，防止未授权者对数据的浏览、篡改和破坏。

2.3 物理设施上的因素

例如水、台风、地震等自然灾害，盗窃、破坏和断电等人为事故，以及电磁幅射和线路非法搭接等技术因素引起的通信设施的损坏。

2.4 人员管理和操作规程上的因素

由于系统管理、维护、操作人员缺乏训练或不可靠而造成系统非法操作、设备受损和通信中断等事故。

由于以上这些不安全因素的影响，会导致基于 GPRS 监控系统的安全运行受到来自不同层面、不同程度的威胁。

3 基于 GPRS 监控系统的安全策略

3.1 GPRS 模块安全策略

3.1.1 访问控制策略

对于暴露在公用网络的 GPRS 模块和网络系统，访问控制是系统安全防范和保护的主要策略，它的主要任务是保证系统资源不被非法使用和非常访问。它也是维护网络系统安全、保护系统资源的重要手段。GPRS 网络对用户的访问控制主要是通过用户身份认证进行的。GPRS 系统的身份认证由移动台、

SGSN 和 HLR/AUC 共同完成，认证是基于移动台和 HLR/AUC 之间的共享密钥 Ki。认证过程如图 1 所示。具体如下：移动台发出接入请求到 SGSN；SGSN 发送认证数据请求消息到 HLR/AUC，请求用户的认证数据；HLR/AUC 首先产生一个随机数 RAND，然后由用户的私钥 Ki 和随机数 RAND，经 A3 算法产生签名响应 SRES，经 A8 算法产生加密密钥 GPRS-Kc，然后将认证向量(RAND，SRES，GPRS-Kc)通过认证数据响应消息，发送到 SGSN；SGSN 向移动台发送认证请求消息，认证请求消息包括从 HLR/AUC 那里接收到的随机数 RAND；移动台利用 SIM 卡存储的密钥 Ki 和接收到的随机数 RAND，经 A3 算法产生签名响应 SRES，经 A8 算法产生会话密钥 GPRS-Kc，然后将签名响应 SRES 通过认证响应消息发送到 SGSN；SGSN 判断从移动台收到的 SRES 是否与从 HLR/AUC 收到的一致，如果一致则认为认证通过，在接下来的通信中移动台和 SGSN 将利用各自的会话密钥 GPRS-Kc 进行加密和解密。

图 1 GPRS 系统的认证过程

3.1.2 信息加密策略

通过信息加密的方式来实现对网络传输数据的保护。在 GPRS 无线接口部分采用 GPRS 加密算法来保证 MS 到 SGSN 之间的安全性。GPRS 的用户信息加密功能是在 LLC 层实现的。GPRS 加密算法有三组输入参数：加密密钥(Kc)；帧参数输入(Input)；传输方向(Direction)。加密算法的输出参数：Output。用户数据和信令数据加解密的流程如图 2 所示，发送端通过加密算法产生密钥流，密钥流与要发送的明文消息逐比特异或产生密文，完成加密过程。密文传到接收端后，由接收端先通过加密算法产生密钥流，然后与接收到的密文逐比特异或产生明文，完成解密过程。

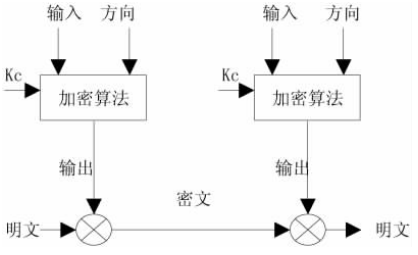

图 2 加密和解密流程

(UI(Unconfirmed Information) frame, Input=((IOV^{UI} (SX)+LFN+OC) mod2^{32}

(I(Information)frame, Input=((IOVI +LFN+OC)mod3^{32}

SX=2^{27} (SAPI+2^{31}

其中 IOV^{UI} 与 IOV^{I} 是由 SGSN 产生的 32bit 随机数；LFN 是 LLC 帧头中的帧(长度为 9bit)，其作用是提供密码同步；OC 是一个二进制计数器，独立于收发两边 (长度 32bit)；SAPI (Service Access Point Identifier,4bits)。

为了正确传递数据，GPRS 服务节点和移动终端中对数据流的加密和解密过程必须保持同步，这在 GPRS 网络通过 LLC 包的序列号以及数据传送方向 (只有从终端到网络或从网络到终端两个方向)来保证。

3.1.3 数据完整性验证策略

完整性证明是在数据传输过程中，验证收到的数据和原来数据之间保持完全一致的证明手段。检查是最早采用数据完整性验证的方法，它虽不能保证数据的完整性，只起到基本的验证作用，但由于它的实现非常简单(一般都由硬件实现)，现在仍广泛应用于网络数据的传输和保护中。近几年来开始使用公钥系统的数字签名等算法，可以保证数据的完整性。

3.2 系统其它模块的安全策略

由于 GPRS 系统的骨干网是基于 IP 的网络，所以 IP 网络的所有安全问题在 GPRS 网络中仍然存在，包括来自内部的安全攻击和来自与 GPRS 网络相连的外部数据网络及其他 GPRS 网络的威胁。因此除了采取上述 GPRS 模块的安全措施外，还应采用针对计算机操作系统的网络病毒防范、系统授权管理、系统自动报警策略、系统安全管理策略等。

3.2.1 网络防病毒策略

网络防病毒技术包括预防病毒、检测病毒和消除病毒等 3 种技术，网络防病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测，工作站上采用防病毒芯片和对网络目录及文件设置访问权限等。在接入 GPRS 网的每个台式机上要安装台式机的反病毒软件，在各专业应用服务器上要安装基于服务器的反病毒软件，在防火墙或网关上要安装基于应用网关的反病毒软件。这些环节彼此相辅相成，通过相互反馈病毒入侵检测信息，及时封堵病毒在 GPRS 网上的传播；同时通过系统中心控制台，集中管理防毒软件在各环节上的自动分发、配置和更新并提供最新疫情信息的自动更新。

3.2.2 系统授权管理策略

用户的权限控制是针对用户非法操作所提出的一种安全保护措施。不同的用户和用户组被赋予相应的权限，指定用户对这些文件、目录、设备能够执行哪些操作；用户权限一般划分为系统管理员权限(Supervisor)、读权限(Read)、写权限(Write)、创建权限(Creat)、删除权限(Delete)、修改权限(Modify)等。通过权限设置可以对系统访问者进行有限管理，系统安全性得到保证。

3.2.3 系统自动报警策略

作为一种远程监控系统，能够在系统运行出现异常时自动报警是必须具备的功能。基于 GPRS 的电力远程监控系统的自动报警主要针对的是电流越线和电缆故障两种异常状况。监控系统实时监测各条线路的电流数据，并设置电流的上限值和下限值，电流一旦越线则触发报警。同时监控系统可以设置电路通断的时间，如果在断开的时间段线路产生电流值或在连接的时间段无电流值，也需要自动报警。电缆防盗是监控终端的重中之重。只要电缆发生任何异常，该终端就会立即向监控中心发送报警信息。目前，常用的电缆防盗报警方法包括检测方法和信号传输方法等。

3.2.4 系统安全管理策略

有效保证系统安全，不仅涉及到技术上的问题，也与系统安全管理息息相关。因此，在采取上述技术措施的同时，加强系统安全管理对保证系统安全将起到十分重要的作用。系统的安全管理具体包括：确定安全管理等级和安全管理范围；制订有关系统操作使用手册；对系统操作人员进行技术培训；制定系统的维护制度和应急措施等。

4 结束语

本文所介绍的电力远程监控系统已在厦门某大桥项目中得到实际运用，并具有高可靠性和实时性。要保证整个监控系统的正常稳定运行以及数据传输安全性，需要在 GPRS 网络模块和计算机系统等方面采取一系列的安全策略。需要强调的是，网络

(下转第 28 页)

I^2C 总线，用户在操作键盘时，产生外中断 3，将键值数据送到 I^2C 总线，读数据保存到键值缓冲寄存器里供读取，置时钟线为高，通知从设备开始接受数据位，主机在接收完每一个数据后，都将产生应答位，最后结束总线。

3.2 人机界面模块

主要是编写液晶屏显示器驱动，在 240＊320 的屏幕上显示字符，汉字和图片信息等，实现过程是要建立 ASCII 字库和汉字库文件，或图像文件，根据要显示的位置以及所显示文字的偏移量显示相应的汉字或字符，然后将所需要的这些功能封装在函数中，以后只需要调用这些函数，便可实现图片，汉字和字符的显示。例如字符和汉字显示函数形式为 void Display_Information(uint x,uint y,uchar *pStr,uint LineColor,uint FillColor,uchar Mod)x，y 表示汉字在屏幕上显示的位置，pStr 是一个指针变量，指向要取的汉字或字符，LineColor 表示汉字颜色，FillColor 表示汉字的背景颜色，Mod 则表示显示模式。

3.3 系统任务调度

各个任务之间都有数据需要交换，我们采用了消息机制进行任务间的通信，多个数据组成消息队列，依次完成数据的传递。图 2 是 μC/OS－Ⅱ控制下的任务状态转换图。在任一给定的时刻，任务的状态一定是在这五种状态之一。睡眠态指任务驻留在程序空间之中，还没有交给 μC/OS－Ⅱ管理。通过调用 OSTaskCreate()函数把任务交给 μC/OS－Ⅱ管理，该任务就进入就绪态准备运行。通过调用 OSStart()进入运行态，这个任务就得到了 CPU 的控制权，运行态的任务通过中断就进入了中断服务态（ISR）。响应中断时，正在执行的任务被挂起，中断服务子程序控制了 CPU 的使用权。中断服务态任务通过调用 OSIntExit()返回到运行态，运行态任务使用权被剥夺则进入到就绪态，就绪态任务通过调用 OSTaskDel()返回到睡眠态。正在运行的任务可能需要等待某一个事件发生通过调用 OsSemPend()实现，如果该事件并未发生，调用上述函数的任务进入了等待态。等待态任务通过调用 OsSemPost()进入就绪态或通过调用 OSTaskDel()回到睡眠态等。这就是任务运行过程。

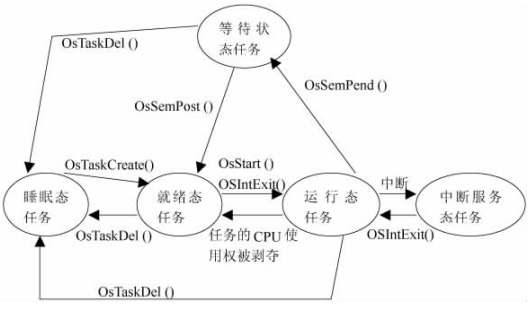

图 2 任务状态转换图

编程装置软件系统首先执行最高优先级的任务，系统进入运行状态，进入到系统主界面。用户通过按键选择不同的菜单功能，系统进入消息循环中等待用户操作。当有按键按下或外设收到某个命令时，其对应的监控扫描任务会向系统发送消息。当消息收到后，随即调用相关函数处理该消息。处理完该消息后，系统进入循环等待下一条消息。

3.4 PLC 指令编译

源程序是设计编译程序的出发点，首先研究源程序的语法和语义及运行模型，研究 PLC 主机，设计目标代码的指令系统，构造编译程序的算法是从研究源程序及目标程序产生的，首先找到源语言的形式描述，根据这种描述，构造出相应的分析加工程序。语言分语法，语义和语用。手持编程器的主要功能就是通过该实验装置完成 PLC 源程序的编译。

源程序编译模块由 PLC 源代码程序、语法分析程序、词法分析程序等三部分组成。PLC 源代码程序根据 PLC 指令格式和规则，辨识指令的操作码和操作数，分别放入一个结构数组变量中，再通过词法分析程序和语法分析程序分析程序两次遍历检验语法语义错误，若出现错误则通过液晶屏显示其错误信息，若无错误，则将源程序转换为目标代码，根据手持编程器实现的编译功能。

3.5 CAN 通讯模块

CAN 总线通讯模块主要包括三个部分：系统初始化、数据发送和数据接收。系统初始化主要包括 CAN 接口初始化。数据的发送包括串口发送程序和 CAN 总线发送程序，数据的接收包括串口接收程序和 CAN 总线接收程序。CAN 通讯发送子程序将从串口接收到的 8 位数据发送到 CAN 总线上。发送节点报文时，用户只需将待发送的数据按规定的格式组合成一帧报文，送入发送缓存区 Send_buffer 中，然后启动 CAN 总线发送即可，在往发送缓存区 Send_buffer 发送报文之前，先要作一些判断，发送程序分发送远程帧和数据帧两种，远程帧无数据域，所以只须发送数据帧。

4 结束语

本课题研究的是一种新型编程器，对以前单任务系统，单片机类型的编程器进行了改进。本文的创新点就是基于嵌入式操作系统实现多任务管理，基于 CAN 总线技术实现远距离对 PLC 主机进行监控和调试，是计算机技术与嵌入式技术进步的结果，符合 PLC 技术进一步网络化，便于研发便携式，低功耗，高性价比，多功能的手持编程器。

参考文献

[1]张嵩，术守喜，丁广乾.基于 ARM 的嵌入式 PLC 的设计[J].自动化与仪器仪表，2008(3)：9－10

[2]饶运涛.现场总线 CAN 原理与应用技术[M].北京：北京航空航天大学出版社，2007：102－108

[3]Jean J.Labrosse.嵌入式实时操作系统 μC/OS－Ⅱ[M].邵贝贝，等，译.北京：北京航天航空大学出版社，2003

[收稿日期：2010.8.23]

（上接第 26 页）

安全是一个系统工程，是单一的产品或技术不可以完全解决的，它涉及到计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种学科，一个完整的安全体系应该是一个由具有分布性的多种安全技术或产品构成的复杂系统，既有技术的因素，也包含人为管理的因素。因此在建立系统安全体系时，用户要结合自己的实际情况和需求来选择相应的技术和产品，制定相关管理条例。

参考文献

[1]文志成.通用无线分组业务：GPRS[M].北京：电子工业出版社，2004

[2]方仁桂，余臻.路灯远程监控系统的报警设计[J].工业控制计算机，2008，21(8)

[3]万子扬.电力系统 GPRS 数据传输安全性研究[J].华中电力，2006(3)

[4]李芬.浅谈基于 GPRS 的电能计量遥测系统的安全策略[J].电测与仪表，2004(8)

[5]沈学利，张美金.计算机安全技术[M].沈阳：东北大学出版社，2002

[收稿日期：2010.12.30]